الردع السيبراني: المفهوم والإشكاليات والمتطلبات

اعداد :

د. رغدة البهي

أستاذ العلوم السياسية بكلية الاقتصاد والعلوم السياسية

جامعة القاهرة (مصر)

ملخص

في السنوات الأخيرة، تزايد عدد الهجمات السيبرانية بشكلٍ حاد. ولذا، بحث الدارسون والمنظرون في قدرة نظريات الحرب الباردة – ومنها نظرية الردع – على التصدي لتلك الهجمات وردعها. ومن هنا تتجلي إشكالية الدراسة، والتي تتمثل في مدى انطباق تلك النظرية على الفضاء السيبراني. يقصد بالردع السيبراني منع الأعمال الضارة ضد الأصول الوطنية في الفضاء. ويرتكز على ثلاثة ركائز هي: مصداقية الدفاع، والقدرة على الانتقام، والرغبة فيه. إذ تدعو الحاجة إلى ردع الهجمات السيبرانية على اختلاف أنواعها وآثارها التدميرية التي لا تطول شبكات المعلومات فحسب، بل تمتد إلى البنية التحتية أيضًا. ولعل ما شهده الواقع المعاصر من حالات متباينة – مثل إستونيا، وجورجيا وكوريا الجنوبية وغيرها – يؤكد ويعزز تلك الحاجة، ولكن لا يمكن إغفال عدد من الإشكاليات التي تواجه الردع السيبراني؛ منها على سبيل المثال: الإسناد، والعقبات القانونية، والفاعلين من غير الدول والمصداقية، وغيرها. تستخلص الدراسة أن متطلبات وشروط نظرية الردع لا تنطبق في الفضاء السيبراني، بعد أن فشلت في تلبية أيا من شروطها؛ نظرًا لاختلاف طبيعة الصراع السيبراني عن مثيله العسكري، ناهيك عن تقويض مفهوم التهديد بالانتقام بسبب مشكلة الإسناد وتحديد المواقع الجغرافية للخصوم. ورغم ذلك، لا يزال الردع السيبراني فعالًا جزئيًا عبر خيارات جديدة، منها الردع السلبي، والاحتجاجات الدبلوماسية، والتدابير القانونية،

والعقوبات الاقتصادية، والانتقام السيبراني أو العسكري وغيرها، وصولًا لبلورة إستراتيجية متكاملة للردع.

الكلمات المفتاحية: نظرية الردع – الردع السيبراني – الهجمات السيبرانية – الفضاء السيبراني –الإسناد

Cyber Deterrence: The Concept, Dilemmas and Requirements

Abstract:

In the recent years, Cyberspace has witnessed a growing number of cyber attacks. That is why many scholars and theorists have questioned the ability of cold war theories – including Deterrence theory – to face and deter those attacks. Thus, the main research problem of this study involves around this ability. Cyber deterrence is intended to prevent harmful acts against national assets in space. It is based on three pillars: the credibility of the defense, the ability to retaliate, and the will to retaliate. Deterring cyber attacks became a must because such attacks are becoming increasingly likely, because they could cause serious damge not only to information networks, but also to the infrastructure as well. The recent contemporary cases – such as Estonia, Georgia, South Korea, etc – confirms and reinforces the need for cyber deterrence, but it's impossible to neglect multiple issues such as: attribution, legal

obstacles, non-state actors, credibility, etc. The study concludes that the cyber deterrence does not meet any of the theory's requirements or conditions. That's because the nature of cyber conflict differes from the military one, the concept of threat retaliation has been undermined, not to mention the attribution problem or the obstacle to define the geographical locations of the opponents. Nevertheless, deterrence is still partially effective by new available options, including: passive deterrence, diplomatic protests, legal measures, economic sanctions, cyber revenge or military attack or others, towards an integrated strategy of deterrence.

Keywords: Deterrence Theory – Cyber Deterrence – Cyber Attacks – Cyber Space – Attribution

مقدمة:

شهد الفضاء السيبراني[1] في السنوات الأخيرة تزايد عدد الهجمات السيبرانية بشكل حاد، نظرًا لتعدد التهديدات السيبرانية لتشمل: الحروب والإرهاب والتجسس الرقمي، وغيرها .ولذا، يصعب تحديد الحجم الحقيقي لتلك الهجمات، وبخاصة أن عديد منها لا يتم التبليغ عنه. ورغم اختلاف غرض وهدف كل منها إلا أن القاسم المشترك بينها هو استغلال ثغرات ونقاط الضعف في المجال السيبراني، بهدف إختراق أجهزة الكمبيوتر وشبكات الحاسوب[2]، حتى تعالت دعوات تطويع الردع كي يتلائم وذلك المجال.

مع الإقرار بخطورة التهديدات السيبرانية، واعتبار الفضاء السيبراني مجالًا للحرب والصراع، بحث خبراء الأمن، والدارسون، وصناع القرار في إستراتيجيات ونظريات الحرب الباردة لاختبار مدى إمكانية تصديها لتلك الهجمات؛ فبدون الردع السيبراني، ستظل البيانات المفتوحة عرضة لأشكالٍ عدة من الاستغلال والاعتداء.

ويثير ذلك إشكاليات وتساؤلات عدة على صعيد نظرية الردع؛ فقواعد الردع لا تتغير بالانتقال من المجالين النووي والتقليدي إلى المجال السيبراني. ويظل الأساس النظري الذي يبنى عليه الردع هو التهديد باستخدام القوة لإقناع الخصم بالامتثال لإرداة الطرف الذي يهدد بها. وبهذا المعنى، يعتمد الردع على ركنٍ ماديٍ ينطوي على تأمين كافة مقتضيات القدرة على إنزال العقاب، وآخر معنوي غايته التأثير النفسي في الخصم من خلال إقناعه بجدوى الانصياع للطرف الذي يهدد باستخدام القوة، وارتفاع تكلفة ما سيقدم عليه من عمل عدائي بالمقارنة بما سيحصل عليه من مكاسب.[3]

وقد بدأ الردع تقليديًا في قواه وأدواته اعتمادًا على وسائل القتال الاعتيادية، وعلى التهديد باستخدام الأسلحة التقليدية. وأكثر أشكال الردع التقليدي شيوعًا هو المتمثل في توعد الخصم بضربة عقابية موجعة في حال حدوث اعتداء من جانبه، وهو ما يسمى

الردع بالعقاب. في حين يقتصر الردع النووي على التلويح باستخدام السلاح النووي سواء أكان هذا الاستخدام جزئيًا أو كاملًا، محدودًا أو شاملًا.[4]

أو بعبارة أخرى، يعتمد الردع على التهديد باستخدام القوة العسكرية، ولا ينطوي على الاستخدام الفعلي لها، بهدف تخويف الخصم، وزرع القناعة لديه بالقدرة على الاقتصاص منه دون أن تتحول النوايا إلى فعل يلحق الأذى به .وهذا الحد الفاصل بين التهديد باستخدام القوة واستخدامها الفعلي هو الذي يشكل معنى الردع وكينونته.[5]

وتتأسس نظرية الردع على عدد من الافتراضات الرئيسية، منها: أن الدول فواعل عقلانية، تستعين بحسابات المكسب والخسارة بشأن متى ولماذا تشن صراعًا، فإذا كانت الخسائر أكبر من المكاسب، سترتدع الدول عن الإقدام عن أي خطوات عدوانية في مواجهة خصومها، وأن الدول كيانات عقلانية تتخذ قرارات عقلانية لحماية مصالحها القومية .[6]فضلًا عن إبلاغ الخصم بشكل قاطع بحتمية معاقبته والانتقام منه في حالة عدم إذعانه. ناهيك عن امتلاك الدولة إمكانات كافية من القوة تتيح لها مواجهة التهديد الذي تمثله الدولة المهاجمة، بل واستعدادها لاستخدام تلك الإمكانيات عند الضرورة.[7]

الأسئلة البحثية وأهداف الدراسة:

يمكن القول أن **السؤال البحثي الرئيسي** الذي تسعى الدراسة للإجابة عنه هو: ما مدى ملائمة نظرية الردع – وتحديدًا الردع السيبراني – لمواجهة الهجمات السيبرانية؟ وفي إطاره، تتمثل **أهداف الدراسة** في الإجابة على **التساؤلات البحثية** التالية:

ما المقصود بالردع السيبراني؟ وما هي طبيعة الهجمات التي يجب ردعها؟ وما طبيعة الإشكاليات التي تواجه ذلك الردع؟ وكيف يمكن تسكينه في إطار نظرية الردع؟ وكيف يمكن رسم خريطة لما شهده الواقع المعاصر من حالات متباينة من الهجمات السيبرانية؟ وما هي القواسم المشتركة بينها؟ وهل يعد الردع الخيار الأمثل لمواجهة التهديدات السيبرانية على المستويين النظري والتطبيقي؟

يدور مغزى كافة تلك الأسئلة حول الإشكاليات المفاهيمية التي تواجه الردع السيبراني، والهدف من وراء ذلك الردع، وحالاته، وجدواه. أخذًا في الاعتبار التغير في سياق الردع بشكل ملحوظ من ناحية، وتعدد الخصوم الواجب ردعهم؛ من الخصم الواحد إلى خصوم مختلفين، لكل منها قدرات مختلفة على تحمل العقاب من ناحيةٍ أخرى.[8]

مفاهيم الدراسة:

ترتكز الدراسة على مفهومين رئيسيين هما الردع بشكلٍ عام والردع السيبراني بشكلٍ خاص، وذلك كما يلي:

التعريف الأبرز والأشهر للردع – والمتداول بكثرة في الأدبيات – هو تعريف الجنرال "أندريه بوفر" الذي عرف الردع بأنه "منع دولة معادية من اتخاذ قرار باستخدام أسلحتها – أو بصورة أعم – منعها من العمل أو الرد إزاء موقف معين باتخاذ مجموعة من التدابير والإجراءات التي تشكل تهديدًا كافيًا حيالها، والنتيجة التي يراد الحصول عليها بواسطة التهديد هي نتيجة سيكولوجية نفسية.[9]"

أما الردع السيبراني فيُعرّف – كما ستوضح الدراسة فيما بعد – بأنه "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء.[10]" وبهذا المعنى، يرتكز الردع السيبراني على ثلاثة ركائز هي مصداقية الدفاع، والقدرة على الانتقام، والرغبة في الانتقام.

الدراسات السابقة:

يمكن تقسيم الدراسات السابقة وفقًا لثلاثة محاور رئيسية، وذلك على النحو التالي:

الاتجاه الأول : يرى عدم جدوى نظرية الردع على صعيد الفضاء السيبراني، مشككًا في جدواها وفعاليتها، فطبيعة العمليات السيبرانية تُقوض من الدور المحتمل للردع، وقد تجعله عديم الفائدة كليًا. ويركز هذا الاتجاه على الإشكاليات التي تواجه الردع

السيبراني، ومنها :صعوبة تحديد هوية مرتكبي الهجمات ابتداءًا، فضلًا عن غياب القوانين اللازمة والرادعة، على نحو يوفر لمرتكبيها الملاذ الآمن، مما يحول دون ملاحقتهم.[11]

الاتجاه الثاني :يرى أن نظرية الردع لا تنطبق فحسب في المجال السيبراني، لكنها ضرورةً أيضًا؛ فبدون الردع السيبراني، ستظل البيانات المفتوحة عرضة لأشكال بدائية وخطيرة من الاستغلال والاعتداء، ومنها سرقة البيانات، وانتهاك حقوق الملكية الفكرية، وتعطيل الأعمال التجارية، وإيقاف تشغيل النظم الحيوية. ذلك أن الردع السيبري لابد أن يكون جزءًا لا يتجزأ من إستراتيجيات الأمن القومي للدول.[12]

الاتجاه الثالث :يرى أن نظرية الردع يمكن أن تتلائم والفضاء السيبراني، ولكن بشروط وضوابط محددة، منها تبني مفهوم واسع للردع، والمزج بين خيارات عدة في سبيل الوصول إلى إستراتيجية متكاملة له، أخذًا في الاعتبار أن الردع في عصر المعلومات يختلف كثيرًا عنه في عصر الحرب الباردة في النوع والنطاق، مما يتطلب نهجًا شاملًا يدمج كل المقومات العسكرية والاقتصادية والاستخباراتية والقانونية، تعزيزًا لأمن المعلومات من ناحية، وخلقًا للردع من ناحية أخرى.[13]

أولًا: مفهوم الردع السيبراني:

يعرف الردع السيبراني على أنه "منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية.[14]" ويرتكز الردع السيبراني على ثلاثة ركائز هي عماد إستراتيجية الدفاع السيبراني، تتمثل في: مصداقية الدفاع Credible Defense، والقدرة على الانتقام An Ability to Retaliate، والرغبة في الانتقام A Will to Retaliate.

الركيزة الأولى – مصداقية الدفاع: يتطلب الدفاع عن أنظمة المعلومات، وردع أي محاولة لاختراقها – من بين متطلبات أخرى – توافر أنظمة نسخ احتياطية Backup Systems، مما يعني أن أي هجوم ناجح عليها، لن يسفر عن التدمير التام لها أو

الفقدان الكلي لما تحويه من معلومات؛ ورغم تزايد تكلفة هذا الحل إلا إنه الحل العملي الأكثر فعالية.

الركيزة الثانية – القدرة على الانتقام: لابد أن يتكبد المهاجم ضررًا يفوق ما وقع على المدافع من أضرار، ولكن هذا يتطلب القدرة على الانتقام وتنفيذ هجمة سيبرانية أو أكثر ضد المهاجم الأصلي، بعد التعرف عليه وهو صعب التحقق.

الركيزة الثالثة – الرغبة في الانتقام: فعلى المدافع أو من تعرض للهجوم أن يعلن عن رغبته في الانتقام من المهاجم، ذلك أن امتلاك القدرة على الانتقام لا تكفي بمفردها لردعه.([15])

ورغم إمكانية تعريف المفهوم، وتحديد ركائزه على المستوى النظري، إلا أن هذا التعريف لا يحظى بإجماع الدول على المستوى العملي، والمثال على ذلك هو الولايات المتحدة والصين؛ ففي الوقت الذي تفضل فيه الولايات المتحدة استخدام مصطلح الأمن السيبراني Cyber Security للتركيز على التكنولوجيات والشبكات والأجهزة الآلية، تفضل دول مثل الصين وروسيا استخدام مصطلح أوسع ألا وهو "أمن المعلومات" Information Security، ليشمل المعلومات التي تمر عبر الشبكات وكذلك التقنيات المعلوماتية. ودون معجم مشترك، سيستمر الخلاف بشأن كيفية استخدام الإنترنت، وسياسات الردع، وطبيعة الهجمات الواجب ردعها.

ثانيًا: الهجمات السيبرانية

تتطلب دراسة الردع السيبراني، التعرض إلى أنواع الهجمات السيبرانية لتحليل طبيعة ما يمكن ردعه منها. فيمكن للهجمات السيبرانية أن تتسبب في دمار هائل يطول الأمن القومي للدول، ويمكنها أيضًا أن تستهدف القيادة السياسية، والأنظمة العسكرية، والمواطنين العزل([16])، وبخاصة أنها تشمل مجموعات كاملة من الأساليب والأدوات التي يمكنها التأثير في الفضاء السيبراني.([17])

يمكن تعريف الهجمات السيبرانية بأنها "فعل يُقوض من قدرات وظائف شبكة الكمبيوتر، لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف ما تُمكن المهاجم من التلاعب بالنظام. [18]"فهدف أنظمة المعلومات هو إتاحة المعلومات وضمان سلامتها. ولذا، تهدف الهجمات السيبرانية – على العكس من ذلك – إلى سرقة المعلومات، أو انتهاك سريتها، أو تعديلها، أو منع الوصول إليها. ولعل أبرز أنواع الهجمات ما يلي:

- **الهجمات السرية**: وتعد أحد أنواع التجسس التقليدي باستخدام وسائل التكنولوجيا الفائقة؛ ولعل معظم الهجمات السيبرانية المتطورة التي أطلقت من قبل الدول القومية أو الجماعات الإجرامية تقع ضمن هذه الفئة. ولكن، لا يمكن تصور الرد بهجوم ساحق أو مدمر على التجسس السيبراني، مهما بلغت تداعياته على الأمن القومي. ودون التهديد برد واسع النطاق، ستهوى الركيزة الأساسية للردع، وسيفشل في منع الهجمات السيبرانية.
- **Integrity Attacks:** تصمم بعض الهجمات لتحقيق ميزة تكتيكية أو إستراتيجية عن طريق تخريب نظم معلومات الخصم المدنية أو العسكرية الهامة. فيمكن أن ينطوي التخريب على التلاعب بالبيانات داخل نظم المعلومات التي يمكن أن تشوه وعي العدو عن طريق نشر معلومات خاطئة داخل أنظمة ذكائه، أو إخفاء أنشطة محددة قد تكون تحت المراقبة. [19]

ج: **Availability Attacks** -هي تلك التي تسعى لإغلاق نظم المعلومات To Bring Information Systems Offline. وتكمن خطورة الهجمات طويلة المدى منها في ما تسببه من أضرار مدمرة على الاقتصاد، بتأثيرها على شبكة الاتصالات أو الكهرباء على سبيل المثال. أما الهجمات قصيرة المدى التي تستهدف جمع المعلومات الاستخبارية، فيمكن أن تحجب قدرة الدولة على رؤية التهديد السيبراني التقليدي أو واسع النطاق من خلال منع المدافعين من الوصول إلى البيانات

أو المصادر الاستخباراتية الحيوية. وهكذا، يمكن أن تشكل تلك التهديدات خطرًا على الأمن القومي، ولذا يجب أن يتم ردعها.[20]

وعلى ضوء ما سبق، ترى الباحثة أن العالم سيشهد مزيدًا من الهجمات السيبرانية في الأعوام القليلة القادمة، وستصبح الأسلحة الهجومية أكثر ضراوة. وبخاصة أن الهجمات السيبرانية يمكنها أن تفعل أشياء لا يمكن للهجمات التقليدية أن تفعلها. ولذلك، النجاح في المجال السيبراني لا يتطلب الدفاع فحسب؛ فالردع لن يكون فعالًا ما لم يتم تبن قدرات سيبرية هجومية.[21]

ثالثًا: أبرز حالات الهجمات السيبرانية:

ساهم عديد من الأحداث الدولية الأخيرة في رفع وعي الدارسين وصناع القرار بشأن التهديدات السيبرانية، مع التركيز على إمكانية انطباق نظرية الردع في هذا المجال.[22]وتتمثل أبرز الحالات فيما يلي:

- **إستونيا – أبريل 2007** :بدأت سلسلة من الهجمات التي يطلق عليها DDoS attacksضد المواقع التي تديرها الحكومة الإستونية، وتسبب الهجوم في عرقلة ولوج المواطنين إلى بعض المواقع مثل موقع الحزب السياسي الذي ينتمي إليه رئيس الوزراء. من جهة أخرى، استُخدمت الروابط التي ترعاها الحكومة في تضليل المستخدمين، وإعادة توجيههم إلى صور للجنود السوفيت، واقتباساتٍ من مارتن لوثر كينج عن محاربة الشر.

ب- جورجيا – أغسطس 2008 :شهدت جورجيا بالتزامن مع حربها ضد روسيا في أغسطس 2008 مجموعة من الهجمات السيبرانية، وإن كان ضررها الفعلي في حده الأدنى، من حجب بعض المواقع المستهدفة. ويتفق معظم المحللين على أن القوميين الروس هم المسئولون عن الهجوم، ولكن دون دليل يذكر.[23]

ج- كوريا الجنوبية والولايات المتحدة يوليو 2009 :تم استهداف مواقع البيت الأبيض، ووكالة الأمن القومي، والإدارة الاتحادية للطيران Federal Aviation administration، ووزارة الخارجية، والخدمة السرية Secret Service، والخزانة، ولجنة التجارة الاتحادية Federal Trade Commission ، فضلًا عن جهاز المخابرات الوطني في كوريا الجنوبية.

وكذلك الهجوم على شركة سوني بيكتشرز الأمريكية في عام 2014، بسبب فيلم من إنتاج هوليوود، عن زعيم كوريا الشمالية كيم يونغ أون .([24])واستخدم فيروس "ستكسنت" – سابقًا- لمهاجمة برنامج إيران النووي في نوفمبر 2007، ويُعتقد أنه من تطوير الولايات المتحدة وإسرائيل، وقد تم اكتشافه في عام 2010.([25])

وفي يوليو 2011، أعلن نائب وزير الدفاع ويليام لين أن أكثر من 24 ألف ملف من ملفات وزارة الدفاع قد سرق. قبل ذلك ببضعة أشهر، تم اختراق إحدى المختبرات العلمية الرئيسية التابعة لحكومة الولايات المتحدة، ولم تعلن الحكومة الأمريكية عن هوية مرتكبي الهجوم.([26])

وفي عام 2012، تم تدمير 35 ألف جهاز كمبيوتر في شركة النفط السعودية "أرامكو"، لتخريب صادرات النفط. وألقت المخابرات الأمريكية اللوم على إيران. وفي عام 2016، هاجم القراصنة إحدى الوكالات الحكومية السعودية، بالإضافة إلى منظمات في قطاعات الطاقة والصناعة والنقل، والهيئة العامة للطيران المدني التي تنظم الطيران السعودي.([27])

وشهد عام 2016، التسلل الروسي إلى خوادم البريد الإلكتروني للجنة الوطنية الديموقراطية، كما تم اختراق البريد الإلكتروني الخاص بجون بوديستا رئيس الحملة الانتخابية الرئاسية لهيلاري كلينتون. وقام وسطاء بتسريب رسائل إلكترونية إلي موقع ويكليكس، وعلى إثرها قامت الولايات المتحدة بطرد 35دبلوماسيًا روسيا.

ويمكن القول في ضوء تلك الحالات، أنه رغم اختلاف غرض وهدف كل حالة من الحالات السابقة، إلا أنه من الواضح أن حجم الهجمات السيبرانية يتزايد بشكل حاد، ولذا يصعب تحديد حجمها الحقيقي وبخاصة أن عديد منها لا يتم التبليغ عنه.[28] وتتمثل القواسم المشتركة بين تلك الحالات في صعوبة تحديد مرتكبي تلك الهجمات على وجه الدقة، وغياب الرد المضاد، كنتيجة لها. والأهم أنها ليست حكرًا على الدول المتقدمة ذات أنظمة المعلومات الهائلة والمتطورة فحسب.

رابعًا: الإشكاليات

تدعو الحاجة إلى ردع الهجمات السيبرانية على اختلاف أنواعها وآثارها التدميرية، ولعل ما شهده الواقع المعاصر من حالات متباينة تطال الدول المتقدمة والنامية على حد سواء، يؤكد ويعزز تلك الحاجة، ولكن إلي أي مدى يمكن ردع تلك الهجمات، وما هي طبيعة التحديات التي تعترض ذلك المدى؟

يمكن إجمال الإشكاليات التي تواجه الردع السيبراني، على النحو التالي:

- **الإسناد**: من شأن الردع السيبراني أن يفشل طالما لم يعلن الجاني رسميًا عن مسؤوليته عن الهجوم؛ فمن الممكن أن يدعي الإرهابيون – على سبيل المثال – مسئوليتهم عن هجوم ما، في توقيت لا يرغب فيه المهاجم الفعلي في الإعلان عن نفسه.[29]

يمكن لأي شخص أن يكون هو الجاني في الهجمات السيبرانية، وبخاصة أن المعدات اللازمة لشن هجوم سيبراني يمكن الوصول لها، وليست مكلفة، ويمكن شنها من أي مكان تتوافر فيه خدمة الإنترنت. فلكي يعمل الردع لابد من أن يقلق المهاجم من كشف هويته، ومن ثم تعرضه للعقاب أو الانتقام، بيد أن صعوبة تحديد مرتكب الهجمات بدقة، قد يسفر عن استهداف طرف ثالث لا علاقة له بالهجوم إبتداءًا، وهو الأمر الذي لا يُضعف فقط من منطق الردع وفلسفته، لكنه يخلق عدوًا جديدًا أيضًا.

فمن الصعب جدًا، وغالبًا ما يكون مستحيلًا إسناد الهجوم السيبراني إلى مرتكبيه بمجرد اكتشافه من خلال الوسائل التقنية وحدها. ولعل استخدام المصادر الاستخباراتية غير السيبرانية التقليديةNon-Cyber Intelligence، يمكن أن يساعد في تحقيق هذا الهدف.([30])

كحد أدنى، يجب تحسين عمليات الإسناد حتى يتم تفعيل الردع. مما يتطلب من المنظمات – على المدى القصير – تحسين قدراتها على جمع ونقل الأدلة الرقمية .أما على المدى الطويل، فلابد من إنشاء خط إنذار مبكر للحرب السيبرانية، مما يتيح الاختيار من بين مجموعة واسعة من أساليب الاستجابة السريعة.([31])

وقصارى القول، أن الشك في تحديد هوية المهاجم سيؤدي إلى انعدام الرغبة في الانتقام أو الرد، وحتى لو وجدت كيفية أو طريقة لتحديد المهاجم على نحو دقيق، ستظل سرية. وبالتالي، لن يرتدع المهاجم عن شن هجوم سيبراني ضد طرف بعينه دون معرفة قدرته على الإسناد بدقة. فعدم التغلب على تلك الإشكالية يعني تكرار الهجمات مرة أخرى دون تعرض المهاجم للعقاب، أو بعبارة أخرى، تحسين سبل الإسناد ضرورة لفعالية الردع.

ب- تجنب الانتقام أو الرد المضاد :يصعب السيطرة على الهجمات السيبرانية أو التنبؤ بها. ولذلك، ستطول المسافة الزمنية بين الهجوم والرد. لذا، قد يبدو – عند تنفيذه – ردًا تعسفيًا لا علاقة له بالحادث الأصلي. وحدوث أي خطأ في مجال الفضاء السيبراني يعني الرد في مجالات أخرى؛ فعلى سبيل المثال، أعلنت روسيا في عام 1998 صراحةً أنها تحتفظ بخيار الرد على الهجوم السيبراني بأي سلاح في ترسانتها، بما في ذلك ترسانتها النووية.

في مواجهة تلك الصعوبات، والشكوك المحيطة بردود فعل المهاجم، قد تختار الدول التخلي عن خيار الرد على الهجمات السيبرانية. مما يُقوض من الرغبة في الانتقام، ومن ثم الردع.([32])

ج- العقبات القانونية :لا يمكن تطبيق القوانين الدولية الراهنة على الهجمات السيبرانية إلا بشكل غير مباشر. فيُجرم القانون الدولي العدوان العسكري، ولكن ماذا عن الهجوم السيبراني الذي أسفر عن انفجار قاعدة عسكرية؟ وهل يحق للدولة – إعمالًا لحقها الأصيل في الدفاع عن النفس – استهداف أهداف عسكرية ضد تلك الدولة أو حتى شن هجوم سيبراني مضاد؟ إلا يزال النقاش دائرًا حول المسائل القانونية المتعلقة بالهجمات السيبرانية. وعليه، قد يبدو الرد الانتقامي عملًا عدوانيًا غير مبرر أو مخالفًا لقواعد القانون الدولي.([33])

د- تدخل الفاعلين من غير الدول :([34])يمكن للفاعلين من غير الدول – بما في ذلك المنظمات الإجرامية والجماعات الإرهابية، والنشطاء السياسيين، وغيرهم – إحداث أضرار كبيرة بدرجات مختلفة .فكثيرًا ما يشن الفاعلون من غير الدول هجمات سيبرانية لتحقيق مكاسب مالية أو لتقويض مصداقية الدول .([35])وهو ما يضفي مزيدًا من التعقيد على الردع السيبراني؛ نظرًا لصعوبة استهداف هؤلاء الفاعلين، مما يدعو للتساؤل عن جدوى الرد الانتقامي، ماذا إذا وُجد هذا الفاعل داخل دولة ما، ووفرت له دولة أخرى الحماية، أيهما يتحمل المسئولية([36])؟!

ه- إرسال رسائل صادقة وواضحة للخصم :بدونها يصبح الردع غير فاعل، بل وتتزايد احتمالات سوء فهمه أو تجاهله، مما يزيد من مخاطر التصعيد والصراع. فالقدرة على الإشارة بوضوح تسمح باستعراض القدرات والنوايا على نحو يتيح خيارات واسعة من الردع، بيد أن الإشارة في العمليات السيبرانية أكثر صعوبة لعدد من الأسباب منها صعوبة الإسناد، فيمكن للدول تطوير قدراتها السيبرانية واستخدامها دون أن يسند إليها أي عمل عدائي. ففي الفضاء السيبراني يمكن أن يساء تفسير تلك الإشارات بسهولة، وقد يتم تجاهلها أو عدم ملاحظتها.([37])

و- الوقت :الوقت وحجم العمليات السيبرانية من العوامل الرئيسية الهامة التي تؤثر على الردع السيبراني؛ فإحدى التحديات الرئيسية التي تواجهها نظرية الردع فى الفضاء السيبراني تتمثل في الكشف عن الهجوم في الوقت المناسب. فنظرًا لطبيعة

الأسلحة السيبرانية، يمكن تطوير واختبار القدرة الهجومية السيبرانية دون وجود إمكانيات فاعلة لردعها. فعلى النقيض من الأسلحة المادية، لا توجد منصات صواريخ أو غواصات يمكنها مراقبة ورصد الهجمات السيبرانية قبل وقوعها.[38]

ز- تآكل مصداقية كل من الردع بالإنكار والعقاب :في الفضاء السيبراني، كلاهما يعانيان من نقص المصداقية؛ فالردع بالحرمان غير مرجح تطبيقه بسبب سهولة امتلاك التكنولوجيا اللازمة لشن الهجمات السيبرانية، وعدم نضوج الأطر القانونية الدولية، وذيوع التصور بأن الهجمات السيبرانية ليست خطيرة بما يكفي كي تستحق الردع في المقام الأول. لذا الردع بالعقاب هو الخيار الأوحد، ولكنه يفتقر إلى المصداقية بسبب التحديات المتمثلة في إسناد الهجوم إلى مرتكبيه .[39]فإنكار إحدى الهجمات لا يعني ردعها، أو تغيير حسابات الخصم أو عدوله عن العدوان.[40]

ح- المصداقية :من بين العوامل التي تؤثر في الردع السيبراني هو ثقة المهاجم في قدرة الدولة على الانتقام والرد. ولكن في المجال السيبراني، الأسلحة السيبرانية خفية وغير مرئية إلى أن يُقدم طرف ما على استخدامها. ولذلك، لا يمكن للمهاجم أن يعرف إذا امتلك الخصم القدرة على الرد أو الانتقام.[41]

وبإعادة صياغة ما سبق، يمكن القول، **أن متطلبات وشروط نظرية الردع لا تنطبق على الردع السيبراني**، بعد أن فشل في تلبية أيا من شروطه؛ فلا يوجد أي صراع بالمعنى العسكري إبتداءًا، ولا يمكن التسليم بافتراض العقلانية الكلاسيكي، لما يلعبه الفاعلون من غير الدول من أدوار في الصراع السيبراني. ناهيك عن تقويض مفهوم التهديد بالانتقام بسبب مشكلة الإسناد وتحديد المواقع الجغرافية للخصوم .فضلًا عما يواجهه مفهوم الضرر غير المقبول من إشكاليات جراء انعدام القدرة على تحديد الأصول التي يمتلكها الخصوم وتعريضها للخطر المتكرر. أما عن المصداقية، فتواجه إشكاليات متعددة جراء عدم وجود قواعد للاشتباك، واحتمال وقوع خسائر مضادة.

ولا يمكن إغفال إحدى أهم مواطن الضعف والقصور التي تعتري مفهوم الردع السيبراني، والتي تتمثل في الاتساع الشديد للمفهوم ليطول مجالًا بأكمله، وهو ما لا يحدث في أي مجال آخر من مجالات الحرب .[42]يشمل الفضاء السيبراني مجالات متعددة مثل: الاتصالات، والتجارة، والأعمال التجارية، والتعليم، والتدريب، وأكثر من ذلك. لذا، بناء إستراتيجية فاعلة للردع في الفضاء السيبراني يتطلب تجاوز الحديث عن المجال ككل إلى الحالات التي يمكن للردع أن يكون فاعلًا فيها.[43]

ورغم ذلك، باحثوا الردع يؤمنون بأن الردع لا يزال يجدي؛ وأنه لا يزال فعالًا جزئيًا، لكنه لا يصل إلى المثالية، لكن وجوده أفضل من عدم وجوده على الإطلاق .[44]كما أن فشل الردع السيبراني – على خلاف الردع النووي – [45]لا يسفر عن دمار شامل محقق. وأيضًا، ما شهده الواقع المعاصر من هجمات سيبرانية يجعل من الضروري البحث في كيفية منعها خشية تكرارها، وبخاصة في ظل سهولة الحصول على الأسلحة السيبرانية وشن الهجمات باستخدامها، وصعوبة تحديد الخطوط الحمراء التي لا يمكن تجاوزها على صعيد تلك الهجمات.[46]

خامسًا: متطلبات الردع

الردع السيبراني صعب التنفيذ، كما أن هناك العديد من العوامل التي يجب أن تحدث لضمان تحقيق النتائج المرجوة منه، منها:

- **تطبيق طرق ووسائل جديدة:**

يتطلب الردع السيبراني تطبيق طرق وأساليب جديدة، وإعادة تكييف مفاهيم الردع التقليدية لتتناسب مع هذا المجال الجديد. فلا يمكن معرفة الهدف من الهجمات دون معرفة من شنها؛ ودون معرفة الخصم وهدفه، لا يمكن للردع أن ينجح، وسرقة المعلومات قد تتكرر مستقبلًا، ودون الرد على ذلك الهجوم لن يكون الردع ممكنًا لتآكل مصداقيته. ولذا تتعدد الخيارات والسبل المقترحة للردع، ولعل منها ما يلي:

الخيار الأول – الردع السلبي :وهو الأقل تعقيدًا، لكنه ليس واقعيًا، إذ يتمثل في عدم الرد على الخصم، ولكن مع الاعتراف بأن الأمن السيبراني، وكافة الإجراءات المتبعة غير كافية، وتطوير الأنظمة الأمنية بشكل مستمر. فمن شأن أي تحسن في تدابير الأمن السيبراني أو الردع السلبي أن يرفع تكاليف أي هجوم سيبراني في المستقبل، مما يقلل من فرص حدوثه. ومع ذلك، سيعتبر المهاجم أن هذا الرد بمثابة دعوة لمواصلة الأنشطة السيبرانية على نطاق أوسع.

الخيار الثاني – الاحتجاجات الدبلوماسية :يمكن طرد مسئولي الدولة التي يشتبه في شنها الهجوم، ومع ذلك، تسرى قواعد المعاملة بالمثل على ذلك الأمر. ومن شأن ذلك أن يضر بسمعة الدولة على الصعيد الدولي، لكنه في المقابل لن يسبب لها ما يكفي من أضرار تردعها عن شن هجمات مستقبلية.

الخيار الثالث – التدابير القانونية :بمعنى اتخاذ إجراءات قانونية ضد الدولة التي يشتبه في شنها الهجوم. ولكن كما هو الحال مع الاحتجاجات الدبلوماسية، التدابير القانونية هي في الغالب ذات طبيعة رمزية، وتنطوي على خطر إقامة دعوى قضائية تضطر فيها الدول لكشف معلومات استخباراتية حساسة، ليسبب ذلك ضررًا أكثر مما يستحق، ولن يكون له تأثير رادع.

الخيار الرابع – العقوبات الاقتصادية :بعد إتهام الولايات المتحدة لكوريا للمشاركة في قرصنة شركة سوني بيكتشرز مثلًا، تم تعزيز العقوبات الاقتصادية ضد النظام الكوري. ومع ذلك، بمجرد تثبيت العقوبات أو تعزيزها، لن يكون لدى الدولة أي سبب وجيه لتغيير سلوكها، ما لم تكن هناك مبادئ توجيهية حول كيفية تخفيف أو التخلص من العقوبات. ناهيك عن التداعيات المحتلة للاعتماد المتبادل، وارتباط اقتصاديات الدول مع بعضها البعض في شبكة مترامية الأطراف، متداخلة المصالح؛ فمن شأن ذلك أن يطول الدول التي تفرض العقوبات أيضًا.

الخيار الخامس – الانتقام في الفضاء الافتراضي :لطالما كان التهديد بالانتقام رادعًا فعالًا يردع الاختراقات السيبرانية المستقبلية. فمن شأن سرقة ونشر معلومات الخصم واستهداف بنيته التحتية أن يكون خيارًا فعالًا. ومع ذلك، يتزايد خطر التصعيد المتبادل.

الخيار السادس – الانتقام العسكري :وهو خيار غير واقعي، لأنه سيسفر عن رد عسكري مضاد، ويمكن أن يبدأ عملية خطيرة من التصعيد. ويبدو هذا الخيار مرجحًا إذا أسفرت الهجمات السيبرانية عن نتائج كارثية، ووفقًا لموازين القوى بين طرفي الصراع .[47]وتكمن الإشكالية في أن التهديد بضربة مضادة، قد لا يكون سريعًا بما يكفى لكي يمنع العدوان. ومع إشكالية الإسناد، قد تصبح الضربة المضادة آلية للرد والدفاع لا الردع.[48]

كل من تلك الخيارات يمثل إشكالية إلى حد ما؛ فجميعها تقريبًا يشترك في خطر التصعيد، وأيا منها قد يعجز عن ردع الهجمات السيبرانية في المستقبل .ولكن إذا لم يتم اتخاذ أي إجراء، فإن مصداقية الأمن السيبراني ستتضاءل.[49]

وفي رؤية الباحثة، تعكس تلك الخيارات حقيقة هامة، تنال من مصداقية الردع، مفادها اللجوء إلى مجالات أخرى بخلاف المجال السيبراني للرد على الهجمات التي تطال ذلك المجال. فنظرًا لصعوبة تحديد المهاجم بدقة، قد لا يلجأ الطرف المتضرر إلى الرد على الهجوم عبر المجال السيبري، ولكن قد يلجأ إلى التهديد باستخدام الأداة العسكرية ردًا عليه، أو قد يقرر استهداف أهداف مناظرة لدى الخصم؛ فإذا تسبب الهجوم السيبراني في تعطيل إمدادات الكهرباء على سبيل المثال، يمكن استهداف مثيلتها لدى الخصم، وإذا تسبب الهجوم السيبراني في ضرر بالغ يهدد الأمن القومي، فيمكن التهديد بتغيير النظام السياسي لدى الخصم أو شن الحرب عليه.[50]

- **بلورة إستراتيجية متكاملة للردع:**

يختلف الردع في عصر المعلومات كثيرًا عنه في عصر الحرب الباردة التي تميزت بقلة عدد الدول المالكة للأسلحة النووية، لكن عدد الدول التي تسعى لتطوير أسلحتها السيبرانية يبلغ 140 دولة، كما أدخلت 30 دولة الوحدات السيبرية في جيوشها.

الحديث عن الردع السيبراني بات أكثر مرونة، وباقترابات مختلفة، وتلك المرونة يمكن تداولها بطريقتين مختلفتين:

الأولى – الأنظمة البديلة: إن اعتماد دولة ما على نظام واحد، وتم اختراقه، سيسفر عن عواقب وخيمة؛ وبخاصة إذا تعلق هذا النظام بالبنية التحتية الرئيسية للدولة. لذلك، يمكن للدول خلق أنظمة بديلة لتكون في حوزة الدولة نفسها أو الدول الصديقة. وفي حالة حدوث هجوم سيبراني، يمكن الاستعانة بتلك الأنظمة البديلة أو الاحتياطية.

الثانية – إعادة التأسيس :فإذا أمكن للدولة التغلب على الهجوم الذي تعرضت له بسرعة، وإعادة تشغيل النظام، ستكون الآثار هامشية .ولكن الطريقة الوحيدة لتجنب الهجوم هي الاحتجاب عن الجميع، ورغم كونه السبيل الأفضل للردع، إلا أنه يكتنفه مسائل قانونية عدة.[51]

خاتمة:

على الردع السيبراني التصدي لمختلف الطرق التي يحدث بها الاختراق، أو تُشن بها الهجمات، ومنها اختراق الأجهزة المستهدفة والشبكات والمعلومات، التي تعتمد على نقاط الضعف التقنية في الشبكات وأجهزة الكمبيوتر. إذ يعتمد عديد من العمليات عن بعد على احتمال أن يستقبل الضحايا رسالة أو ملف يتضمن برنامجًا ضارًا يهدد أنظمتها بشكل غير مقصود.[52]

يظل من الهام ردع الهجمات السيبرية؛ فلا يزال الردع ضروريًا ومناسبًا، ولكن النظرية الكلاسيكية للردع لم تعد كافية .[53]لذا يجب تبني مفهوم واسع من الردع يستخدم نهج Whole-of-Government لدمج كل عناصر السلطة الوطنية،

الدبلوماسية والعسكرية والاقتصادية، والاستخباراتية، والقانونية، لتعزيز أمن المعلومات وخلق حالة من عدم اليقين في أذهان الأعداء حول فعالية أي نشاط سيبراني، وزيادة تكلفته وعواقبه.

فلابد من نشر دفاعات قوية والاعتماد على أنظمة مرنة يمكن أن تتعافى سريعًا من الهجمات أو أي اضطراباتٍ أخرى. تلك التدابير لابد أن تتأسس على القدرة والرغبة في الرد على الهجمات السيبرانية من خلال جميع الوسائل اللازمة، على نحو يتسق والقانون الدولي. بحيث لا تقتصر تلك التدابير على متابعة تدابير إنفاذ القانون، بل تشمل فرض عقوبات على المهاجمين وشن عمليات سيبرانية هجومية ودفاعية، واستنفاد جميع الخيارات المتاحة لاستخدام القوة العسكرية.[54]

إستراتيجية الردع الفعالة يجب أن تتضمن الإعلان عن استجابة واستعراض قدرات استجابة فاعلة مثل: فرض العقوبات، وتطوير ونشر قدرات دفاعية لمنع نجاح أي هجوم محتمل، فضلًا عن إنشاء قوات متخصصة للمهمات السيبرانية، وتطوير وتعزيز البنية التحتية العسكرية والتجارية الهامة لكي تصد أي هجوم محتمل، ناهيك عن تعزيز وتطوير الاستخبارات لاكتشاف هوية المهاجم. ولا يكفي لتلك الإستراتيجية الاعتماد على القدرات السيبرانية أو النووية فحسب، بل يتطلب الأمر الاعتماد على الأسلحة غير النووية، على نطاق واسع، مثل :الضربات التقليدية والدفاع الصاروخي، والفضاء الهجومي.

وكذا، تشديد الإجراءات القانونية الرادعة التي تحول دون التسبب في أضرار عابرة للحدود تتبع سيادة الدولة أو ولايتها القانونية، بل ومحاسبتها حال فشلها في وضع تدابير تنظيمية لردع الهجمات السيبرانية داخل أراضيها. إن وضع قوانين للجرائم السيبرانية يعد خطوة كبرى نحو التصدي لها؛ فكل دولة عليها واجب اتخاذ التدابير المعقولة والمناسبة لتأمين مجتمع المعلومات، من خلال وضع تدابير قانونية لضمان أمن وفعالية شبكات الاتصالات الدولية. وهذا يؤكد المسئولية الجماعية للدول عن الأمن السيبراني.[55]

وقصارى القول، أن طبيعة العمليات السيبرانية تُقوض من الدور المحتمل للردع، وقد تجعله عديم الفائدة كليًا. ورغم ذلك، تتزايد أهميته في ظل هشاشة الدول في الاستجابة للهجمات السيبرانية من ناحية، وقدرته على ردع بعض الفاعلين من ناحية أخرى. ولكنه إجمالًا لن يكون فعالًا تمامًا.

قائمة المراجع

أولًا – المراجع باللغة العربية:

- **الكتب:**
- إسماعيل صبري مقلد، *العلاقات السياسية الدولية دراسة في الأصول والنظريات*، القاهرة: المكتبة الأكاديمية، 2010
- أندريه بوفر، *الردع والإستراتيجية*، ترجمة: أكرم ديري، بيروت: دار الطليعة للطباعة والنشر، 1970
- برونو تيرتري، *السلاح النووي بين الردع والخطر*، ترجمة: عبد الهادي الإدريسي، الإمارات العربية المتحدة: هيئة أبو ظبي للثقافة والتراث (كلمة)، 2011
- عبد القادر محمد فهمي، *النظريات الجزئية والكلية في العلاقات الدولية*، عمان: دار الشروق للنشر والتوزيع، 2010
- **المواقع الإلكترونية على شبكة المعلومات:**

1-العربية سكاي نيوز، ستكسنت فيروس ضد إيران، فبراير 2013، متاح على:

http://www.skynewsarabia.com/web/article/114276/%D8%B3%D8%AA%D9%83%D8%B3%D9%86%D8%AA-%D9%81%D9%8A%D8%B1%D9%88%D8%B3-%D8%B6%D8%AF-%D8%A7%D9%95%D9%8A%D8%B1%D8%A7%D9%86

تاريخ الاطلاع 2017/2/1

-2 العربية سكاي نيوز، تفاصيل الهجوم .. قراصنة يدمرون كومبيوترات في وكالة الطيران السعودي.. ويستبدلون البيانات بصورة الطفل السوري آلان كردي، متاح على:

http://www.skynewsarabia.com/web/article/114276/%D8%B3%D8%AA%D9%83%D8%B3%D9%86%D8%A%D9%81%D9%8A%D8%B1%D9%88%D8%B3-%D8%B6%D8%AF-%D8%A7%D9%95%D9%8A%D8%B1%D8%A7%D9%86

تاريخ الاطلاع 2017/2/1

ثانيًا – المراجع باللغة الإنجليزية:

- **Documents:**
- The Department of Defense, Cyber Strategy, April 2015, Available at:

https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

- **Books:**

- Krepon, Michael & Julia Thompson (Eds.), *Anti-Satellite Weapons, Deterrence and Sino-American Space Relations*, United States: Stimson Center, September 2013
- Libicki, Martin C., *Cyberdeterrence and Cyber War*, Santa Monica, CA: Rand, 2009
- Morgan, Patrick M., & James J. Wirtz (eds.), *Complex Deterrence Strategy in the Global Age*. United States: The University of Chicago Press, 2009

- **Periodicals:**

1. Brenner, Susan W. & Leo L. Clarke, Civilians in Cyberwarfare: Casualties, *SMU Science & Technology Law Review,* 13, 2010, pp. 1-33
2. Deadening, Dorothy, Rethinking the Cyber Domain and Deterrence, *JFQ*, 2nd Quarter 2015, pp. 8-15
3. Elliott, David, Deterring Strategic Cyber Attack," *IEEE Security & Privacy*, September- October 2011, pp. 36-40
4. Geers, Kenneth, The Challenge of Cyber Attack Deterrence, *Computer Law & Security Review,* 26, 2010, pp. 298-303.
5. Glaser, Charles L., Deterrence of Cyber Attacks and U.S. National Security, *Report GW-CSPRI*, June 2011, pp. 1-8
6. Harknett, Richard J.& John P. Callaghan & Rudi Kauffman, Leaving Deterrence Behind: War-Fighting and National Cybersecurity, *Journal of Homeland Security & Emergency Management*, Vol. 7, No. 1, 2010, pp. 1-27.
7. Herpig, Sven, Strategic Operations in the Cyber Domain and their Implications for National Cyber Security, *GI-Jahrestagung*, 2015, pp. 597-607

https://www.clingendael.nl/sites/default/files/deterrence_as_a_security_concept_against_non_traditional_threats.pdf

8. Iasiello, Emilio, Is Cyber Deterrence an Illusory Course of Action?, *Journal of Strategic Security,* 7, No. 1, 2013, pp. 53–67.
9. Jensen, Eric Talbot, Cyber Deterrence, *Emory International Law Review* 26, 2012, pp. 1-52
10. Libicki, Martin C., Deterrence in Cyberspace, *High Frontier*, 5, No. 3, May 2009, pp. 15–20

11. Limnéll, Jarno, Offensive Cyber Capabilities are Needed Because Of Deterrence, *The Fog of Cyber Defence*, No. 200, 2013, 200-207
12. Lotrionte, Catherine, A Better Defense: Examining the United States New Norms-Based Approach to Cyber Deterrence, *Georgetown Journal of International Affairs*, 2013, pp. 71-84
13. Lynn, William J., III, The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack, *Foreign Affairs*, September 2011, Available at:

https://www.foreignaffairs.com/articles/2011-09-28/pentagons-cyberstrategy-one-year-later

14. Orji, Uchenna Jerome, Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States, *Defence against Terrorism Review*, Vol. 6, No. 1, Spring & Fall 2104, pp. 31-46
15. Putten, Frans-Paul Van Der, Minke Meijnders & Jan Rood, Deterrence as a Security Concept against Nontraditional Threats, *Clingendael Monitor*, 2015, pp. 1-64, Available at:

https://www.clingendael.nl/sites/default/files/deterrence_as_a_security_concept_against_non_traditional_threats.pdf

16. Solomon, Jonathan, Cyber Deterrence between Nation-States: Plausible Strategy or a Pipe Dream?, *Strategic Studies Quarterly* 5, No. 1, Spring 2011, Available at:

http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA538310

17. Stevens, Tim, A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy*, Vol. 33, No, 1, 2015, pp. 148–170.
18. Todd, Graham H., Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition, *Air Force Law Review*, 64, No. 96, 2009, p. 65
19. Wilner, Alex S., Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism, *Journal of Strategic Studies*, Vol. 34, No. 1, February 2011, pp. 3–37.

www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later

- **Thesis and Dissertation:**

- Beeker, Kevin R., Strategic Deterrence in Cyberspace, Practical Application Graduate Research Project Presented to the Faculty Department of Electrical & Computer Engineering Graduate School of Engineering and Management Air Force Institute of Technology *Air Education and Training Command in Partial Fulfillment of the Requirements for the Degree of Master of Cyber Warfare*, 2009
- Mokarram, Ali, European Cyber Security: A Cyber Deterrence Approach, *Bachelor's Thesis*, University of Twente, 2013, Available at:

http://essay.utwente.nl/63779/1/Mokarram,_2013.pdf

- **Conference Papers:**

- Alperovitch, Dmitri, Towards Establishment of Cyberspace Deterrence Strategy, In: Cyber Conflict ICCC, *2011 3rd International Conference*, Tallinn, Estonia, June 2011
- Kaminski, Ryan T., Escaping the Cyber State of Nature: Cyber Deterrence and International Institutions, In: C. Czosseck & K. Podins (eds.), *Conference on Cyber Conflict Proceedings*, 2010, Tallinn, Estonia, 2010

- **Reports and Studies:**

- Lewis, James A., Deterrence in the Cyber Age, *Center for Strategic and International Studies*, November 2014
- Meer, Sico van Der & Franc Paul Van Der Pulten, U.S. Deterrence against Chinese Cyber Espionage the Danger of Proliferating Covert Cyber Operations, *Nether Lands Institute of International Relations*, September 2015
- Report on Cyber Deterrence Policy, Available at:

http://1yxsm73j7aop3quc9y5ifaw3.wpengine.netdna-cdn.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf

- Haylen Cohen, *The Approaches and Limitations of Cyber Deterrence*, Fall 2005, http://www.cs.tufts.edu/comp/116/archive/fall2015/hcohen.pdf

- **Electronic Resources:**

- Chertoff , Michael & Frank J. Cilluffo, A Strategy of Cyber Deterrence, Available at: https://static1.squarespace.com/static/54cd5aa2e4b0c

656a63a21ce/t/565de2f1e4b03071352aa420/1448993521823/chapter-20.pdf, Accessed at: 1/2/2017

- Meer, Sico Van Der, Deterrence as a Security Concept Against Cyber Threats: 38-43, Available at:

https://www.clingendael.nl/pub/2015/clingendael_monitor_2015_en/2_deterrence_as_a_security_concept_against_non_traditional_threats/pdf/appendix_2_cyber.pdf, Accessed at: 1/2/2017

[1] ((هناك عدد من الترجمات العربية لمصطلح Cyber منها المعلوماتي، والافتراضي، والسيبراني، والرقمي، والافتراضي، إلا أن الباحثة تميل إلى استخدام لفظ "سيبراني" بوصفه الترجمة الأقرب إلى الكلمة الإنجليزية

([2]) Sico Van Der Meer, Deterrence as a Security Concept Against Cyber Threats, Available at:

https://www.clingendael.nl/pub/2015/clingendael_monitor_2015_en/2_deterrence_as_a_security_concept_against_non_traditional_threats/pdf/appendix_2_cyber.pdf, Accessed at: 1/2/2017

And: Frans-Paul Van Der Putten, Minke Meijnders & Jan Rood, Deterrence as a Security Concept against Nontraditional Threats, *Clingendael Monitor*, 2015, Available at:

https://www.clingendael.nl/sites/default/files/deterrence_as_a_security_concept_against_non_traditional_threats.pdf

([3])عبد القادر محمد فهمي، *النظريات الجزئية والكلية في العلاقات الدولية*، عمان: دار الشروق للنشر والتوزيع، 2010، ص ص. 115-117

[4] ((برونو تيرتري، *السلاح النووي بين الردع والخطر*، ترجمة: عبد الهادي الإدريسي، الإمارات العربية المتحدة: هيئة أبو ظبي للثقافة والتراث (كلمة)، 2011، ص ص. 43-47

([5]) عبد القادر محمد فهمي، مرجع سبق ذكره، ص ص. 115-117

([6]) T. V Paul, Complex Deterrence an Introduction, In: T.V. Paul, Patrick M. Morgan, & James J. Wirtz (eds.), *Complex Deterrence Strategy in the Global Age*. United States: the University of Chicago Press, 2009, p. 5.

([7])إسماعيل صبري مقلد، *العلاقات السياسية الدولية دراسة في الأصول والنظريات*، القاهرة: المكتبة الأكاديمية، 2010، ص ص. 514 -515

([8]) James A. Lewis, Deterrence in the Cyber Age, *Center for Strategic and International Studies*, November 2014, p. 18.

[9] ((أندريه بوفر، *الردع والإستراتيجية*، ترجمة: أكرم ديري، بيروت: دار الطليعة للطباعة والنشر، 1970، ص. 31

([10]) Michael Krepon, Space and Nuclear Deterrence, In: Michael Krepon & Julia Thompson (Eds.), *Anti-Satellite Weapons Deterrence and Sino-American Space Relations*, United States: Stimson Center, September 2013, p. 15

([11]) Uchenna Jerome Orji, Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States, *Defence against Terrorism Review*, Vol. 6, No. 1 Spring & Fall 2104, pp. 31-46; Jensen, Eric Talbot, Cyber Deterrence, *Emory International Law Review*, No. 26, 2012, pp. 1-52; Martin C. Libicki, *Cyberdeterrence and Cyber War*, Santa Monica, CA: RAND, 2009; Martin C. Libicki, Deterrence in Cyberspace, *High Frontier*, Vol. 5, No. 3, May 2009, pp. 15–20; Jonathan Solomon, Cyber

Deterrence between Nation-States: Plausible Strategy or a Pipe Dream?, *Strategic Studies Quarterly*, Vol. 5, No. 1, Spring 2011, Available at:

http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA538310; Emilio Iasiello, Is Cyber Deterrence an Illusory Course of Action?, *Journal of Strategic Security*, Vol. 7, No. 1, 2013, pp. 54–67.

([12]) The department of Defense Cyber Strategy, April 2015, Available at:

https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf; Haylen Cohen, *The Approaches and Limitations of Cyber Deterrence*, Introduction to Computer Security, Fall 2005, pp. 1-11

http://www.cs.tufts.edu/comp/116/archive/fall2015/hcohen.pdf

([13]) Kevin R. Beeker, Strategic Deterrence in Cyberspace: Practical Application, Graduate Research Project Presented to the Faculty Department of Electrical & Computer Engineering Graduate School of Engineering and Management, *Air Force Institute of Technology Air Education and Training Command in Partial Fulfillment of the Requirements for the Degree of Master of Cyber Warfare*, 2009, p. 7; *Report on Cyber Deterrence Policy*, Available at:

http://1yxsm73j7aop3quc9y5ifaw3.wpengine.netdna-cdn.com/wp-content/uploads/2015/12/Report-on-Cyber-Deterrence-Policy-Final.pdf

([14]) Michael Krepon, Space and Nuclear Deterrence, In: Michael Krepon & Julia Thompson (Eds.), *Anti-Satellite Weapons, Deterrence and Sino-American Space Relations*, United States: Stimson Center, September 2013, p. 15

([15]) MAJ Lee Hsiang Wei, The Challenges of Cyber Deterrence, *Journal of the Singapore Armed Forces*, Vol. 41, No. 1, 2015, p. 13

([16]) Kenneth Geers, The Challenge of Cyber Attack Deterrence, *Computer Law & Security Review*, No. 26, 2010, pp. 298-303.

([17]) Dorothy Deadening, Rethinking the Cyber Domain and Deterrence, *JFQ*, 2015, 2nd Quarter, pp. 8-15

([18]) MAJ Lee Hsiang Wei, *Op.cit*, pp. 13-22.

([19]) Dmitri Alperovitch, Towards Establishment of Cyberspace Deterrence Strategy, In: *Cyber Conflict ICCC, 2011 3rd International Conference*, Tallinn, Estonia, June 2011, pp. 89- 90

([20]) *I Bid*, p. 90

([21]) Jarno Limnéll, Offensive Cyber Capabilities are Needed Because of Deterrence, *The Fog of Cyber Defence*, No. 200, 2013, pp. 200-207

([22]) Catherine Lotrionte, A Better Defense: Examining the United States New Norms-Based Approach to Cyber Deterrence, *Georgetown Journal of International Affairs*, 2013, pp. 71-84

([23]) Ryan T. Kaminski, Escaping the Cyber State of Nature: Cyber Deterrence and International Institutions, In:

C. Czosseck & K. Podins (eds.), *Conference on Cyber Conflict Proceedings*, 2010, Tallinn, Estonia, 2010, pp. 80-94.

([24]) *I Bid*, pp. 81- 94

([25]) العربية سكاي نيوز، ستكسنت فيروس ضد إيران، فبراير 2013، متاح على:

http://www.skynewsarabia.com/web/article/114276/%D8%B3%D8%AA%D9%83%D8%B3%D9%86%D8%AA-%D9%81%D9%8A%D8%B1%D9%88%D8%B3-%D8%B6%D8%AF-

تاريخ الاطلاع 2017/2/1

([26]) Eric Talbot Jensen, *Op.cit*, pp. 1-52

([27]) العربية سكاي نيوز، تفاصيل الهجوم.. قراصنة يدمرون كومبيوترات في وكالة الطيران السعودي.. ويستبدلون البيانات بصورة الطفل السوري آلان كردي، متاح على:

http://www.skynewsarabia.com/web/article/114276/%D8%B3%D8%AA%D9%83%D8%B3%D9%86%D8%AA-%D9%81%D9%8A%D8%B1%D9%88%D8%B3-%D8%B6%D8%AF-%D8%A7%D9%95%D9%8A%D8%B1%D8%A7%D9%86

تاريخ الاطلاع 2017/2/1

([28]) Sico Van Der Meer, *Op.cit*, pp. 38

([29]) Sven Herpig, Strategic Operations in the Cyber Domain and their Implications for National Cyber Security, *GI-Jahrestagung*, 2015, pp. 597-607.

([30]) Dmitri Alperovitch, *Op.cit*, pp. 87-94

([31]) Kenneth Geers, *Op.cit*, pp. 298-303.

([32]) MAJ Lee Hsiang Wei, *Op.cit*, p. 13

([33]) *I bid*, pp. 13-22

([34]) Susan W. Brenner & Leo L. Clarke, Civilians in Cyberwarfare: Casualties, *SMU Science & Technology Law Review*, No. 13, 2010, p. 249; Graham H. Todd, Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition, *Air Force Law Review*, Vol. 64, No. 96, 2009; William J. Lynn, III, The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack, *Foreign Affairs*, September 2011, available at:

https://www.foreignaffairs.com/articles/2011-09-28/pentagons-cyberstrategy-one-year-later

([35]) Michael Chertoff & Frank J. Cilluffo, A Strategy of Cyber Deterrence, Available at:

https://static1.squarespace.com/static/54cd5aa2e4b0c656a63a21ce/t/565de2f1e4b03071352aa420/1448993521823/chapter-20.pdf, Accessed 1/2/2017

([36]) MAJ Lee Hsiang Wei, *Op.cit*, pp. 13-22.

([37]) Emilio Iasiello, *Op.cit*, pp. 54–67.

([38]) Dmitri Alperovitch, *Op.cit*, 87- 94

([39]) Kenneth Geers, *Op.cit*, pp. 298-303.

([40] (Richard J. Harknett & John P. Callaghan & Rudi Kauffman, Leaving Deterrence Behind: War-Fighting and

National Cybersecurity, *Journal of Homeland Security & Emergency Management*, Vol. 7, No. 1, 2010, p. 17.

([41] (Haylen Cohen, *Op.cit*, pp. 1-11

[42])) فلا يوجد مفاهيم من قبيل: Land Deterrence أو See Deterrence أو Air Deterrence أو Space Deterrence.

([43]) Dorothy E. Denning, *Op.cit*, pp. 8-15

([44]) Tim Stevens, A Cyberwar of Ideas? Deterrence and Norms in Cyberspace, *Contemporary Security Policy*, Vol. 33, No, 1, 2015, pp. 148–170.

([45])قارن بعض المؤلفون الردع النووي مع الردع السيبراني، ووجدوا أن المبادىء التي جعلت من الردع النووي فعالًا لأكثر من نصف قرن تفشل في الفضاء السيبراني. ولمزيد من التفاصيل انظر:

David Elliott, Deterring Strategic Cyber Attack, *IEEE Security & Privacy*, September- October 2011, pp. 36–39.

([46]) Alex S. Wilner, Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism, *Journal of Strategic Studies*, Vol. 34, No. 1, February 2011, pp. 3–37.

([47]) Sico van Der Meer & Franc Paul Van Der Pulten, U.S. Deterrence against Chinese Cyber Espionage the Danger of Proliferating Covert Cyber Operations Nether Lands Institute of International Relations, September 2015, pp. 1-7.

([48]) Eric Talbot Jensen, *Op.cit*, pp. 1-52

([49]) Sico Van Der Meer & Franc Paul Van Der Pulten, *Op.cit*, pp. 1-7.

([50]) Charles L. Glaser, Deterrence of Cyber Attacks and U.S. National Security, *Report GW-CSPRI*, June 2011, p. 5

([51]) Haylen Cohen, *Op.cit*, pp. 1-11

([52]) Report on Cyber Deterrence Policy, *Op.cit*, Electronic Resource

([53]) Haylen Cohen, *Op.cit*, pp. 1-11

([54]) Report on Cyber Deterrence Policy, *Op.cit*, Electronic Resource

([55]) Uchenna Jerome Orji, *Op.cit*, pp. 31-46